AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
ELECTRONIC DEVICE: SAMSUNG GALAXY, IMEI 357157887221312
CURRENTLY LOCATED AT Española Police Department, Española, New Mexico

Case No. **22 MR 1228**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See attachment A, which is incorporated by reference.

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B, which is incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §1951	Interference with Commerce by Threats and Violence (Hobbs Act)
18 U.S.C. §§922(g)(1) and 924	Felon in Possession of a Firearm

The application is based on these facts:

See attached affidavit, which is incorporated by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Emily Fertitta Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: August 19, 2022

Judge's signature

City and state: Albuquerque, NM

Hon. Jerry H. Ritter, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF ELECTRONIC DEVICE: SAMSUNG GALAXY, IMEI 357157887221312	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Emily Fertitta, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), currently assigned to the Albuquerque Division, Santa Fe Resident Agency. I have been so employed since May 2018. During my employment with FBI, I have conducted numerous investigations for suspected violations of federal law, including participation in numerous violent crime investigations. I have received training in how to conduct complex investigations and I have conducted the execution of search warrants on digital media in the past. I have gained substantial experience in these kinds of investigations through formal and on-the-job training, everyday work experience and consulting with other Special Agents

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Samsung Galaxy, IMEI 357157887221312, cracked screen black/dark gray color, hereinafter the "Device." The Device is currently located at the Espanola Police Department, 1316 Calle Adelante, Espanola, NM 87532.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

MARTINEZ BACKGROUND

6. On August 9, 2022, at approximately 08:04 a.m., Española Police Department (EPD) officers responded to an armed robbery call at the Dande Burger Restaurant located at 424 North Riverside Drive, Española, New Mexico (NM) 87532 The UNSUB approached the counter, brandished what appeared to be a firearm described as a silver in color revolver, and demanded money from an employee. The UNSUB robbed $160.00 United States dollars (USD) in currency from the cash drawer and left on foot.

7. Officers reviewed the surveillance footage from the restaurant, and it depicted that the robbery occurred at approximately 05:46 a.m. by an unknown male subject (UNSUB) that wore a grey shirt, light blue "And 1" shorts, white shoes, a camouflage face mask, and a gray hat with a marijuana logo. The UNSUB also had a distinct tattoo of a woman on the inside of the left forearm and another distinct tattoo on the right forearm.

8. Later, on August 12, 2022, EPD officers obtained photographs of RICKY EDDIE MARTINEZ JR's (hereinafter MARTINEZ) tattoos from United States Marshals Service (USMS) and Adult Probation and Parole Office records, and discovered they were

consistent with the UNSUB's tattoos. Officers also know MARTINEZ is a convicted felon from these records.

9. On August 10, 2022, at approximately 05:40 p.m., EPD officers responded to an armed robbery call at the Shell gas station located at 509 South Riverside Drive, Española, NM 87532. Upon arrival, officers learned from the counter employee that the UNSUB entered the gas station's store, walked to the front counter to purchase a candy bar, and began to talk to the employee. During their interaction, the UNSUB pulled out what appeared to be a firearm described as a silver revolver with his right hand, to which the employee reacted by giving the UNSUB cash from the drawer. The UNSUB robbed $352.00 USD in currency from the drawer and left on foot.

10. The employee described the UNSUB as Hispanic, approximately five feet with six inches in height, wore a black shirt, black bandana, and grayish-tannish pants.

11. On August 11, 2022, at approximately 09:33 p.m., EPD officers responded a call regarding an UNSUB with a firearm at Walgreens located at 1114 North Riverside Drive, Española, NM 87532. Upon arrival, officers learned that the UNSUB entered the store, brandished what appeared to be a firearm described as a silver revolver, and demanded money. When the employee was unable to open the cash register in the liquor department and attempted to open the next register, the UNSUB became agitated and fired a round in the direction of the employee. The projectile hit the shelf and wall in the background and the employee sustained burns on the left arm due to the proximity to the firearm's powder. The UNSUB walked behind the counter, grabbed the register, ripped its cords, and left on foot. The employee identified the UNSUB as MARTINEZ because he said they grew up together in Chimayo, NM, and that MARTINEZ had ties with the employees' family members and friends

12. On August 13, 2022, at approximately 12:00 a.m., EPD officers responded to an armed robbery call at 420 Emporia Smoke Shop located at 527 North Riverside Drive, Española, NM 87532. Upon arrival, officers learned that an UNSUB brandished what appeared to be a firearm described as a silver in color revolver, robbed an unknown amount of cash and left in a white Toyota Tacoma pick-up truck.

13. On August 14, 2022, at approximately 2:55 p.m., Taos Police Department (TPD) officers responded to an armed robbery call at Chalupp's Pizza restaurant located at 108 Siler Rd, Taos, NM 87571. Upon arrival, officers learned from the counter employee that an UNSUB entered the restaurant, asked for a large pizza, and stated, "give me the money". Since the employee did not react to the demand, the UNSUB stated, "give me the fucking money", and pulled out what appeared to be a firearm described as a silver revolver with his right hand. The employee opened the drawer, and the UNSUB began taking money out of it. Another employee noticed what was happening and grabbed the UNSUB's left hand to stop the robbery. The UNSUB reacted by firing a round in the direction of the employee and left on foot. TPD officers also learned from interviewing witnesses nearby the restaurant that a white Toyota Tacoma pick-up truck drove pass them shortly after the robbery occurred.

14. On August 15, 2022, at approximately 08:37 a.m., EPD officers responded to an armed robbery call at Family Dollar located at 745 North Riverside Drive Suite G, Española, NM 87532. Upon arrival, officers learned that at approximately 07:00 a.m., an UNSUB brandished a firearm, fired a round towards one of the employees, robbed $15.00 USD in currency, and a pack of lighters. Officers also learned through surveillance footage from a nearby residence that, at approximately 07:16 a.m., the UNSUB ran through the nearby

residence's yard, entered a white Toyota Tacoma pick-up truck parked approximately 300 yards from Family Dollar, and left the scene.

15. Officers believe MARTINEZ committed the robberies committed on August 12, 13, and 14 because the *modus operandi* used to commit them, the presence of the silver revolver, and the presence of the white Toyota Tacoma, as discussed more below.

16. On August 16, 2022, at approximately 9:45 p.m., EPD officers responded to an attempted robbery and homicide call at Blake's Lotaburger located at 206 North Paseo De Onate, Española, NM 87532. Through a series of witness interviews, EPD officers and FBI SAs learned that, at approximately 9:30 p.m., an UNSUB entered the restaurant. While placing a food order with the employee at the counter, the UNSUB brandished what appeared to be a firearm described as a silver .380 revolver, stated "give me the fucking money", fired one round that hit the employee on the chest, jumped over the counter, and pistol whipped another employee six times in the back of head. The UNSUB then attempted to breach the cashier's drawer but was unsuccessful and left the restaurant on foot. FBI SAs reviewed scene of the crime and observed behind the counter one male deceased and one silver revolver bearing the description "AMADEO ROSSI S.A.".

17. SAs interviewed C.G. who was pistol whipped on the head by the UNSUB. C.G. strongly believed that the UNSUB was MARTINEZ based on the UNSUB's eyes, skin color, and height. Through social media and public news, C.G. was aware what MARTINEZ looked like and that he was wanted for seven recent robberies in Española, NM.

18. On August 17, 2022, MARTINEZ was arrested at approximately 5:45 p.m. by the United States Marshals Service in Santa Fe, New Mexico.

FERNANDEZ BACKGROUND AND ASSOCIATION WITH MARTINEZ

19. On August 15, 2022, an EPD officer in an unmarked vehicle, observed a white Toyota Tacoma pick-up truck that matched the description of the vehicle suspected to have been used during the robberies (as stated in paragraphs 7, 8, and 9), and noted that it was bearing NM license plate ACXD48.

20. On August 16, 2022, New Mexico State Police officers located the white Toyota Tacoma pick-up truck bearing license plate ACXD48 and conducted a traffic stop. Chelsea Priscilla Fernandez (herein after FERNANDEZ) was one of the occupants in the vehicle and was read Miranda Rights before being interviewed. FERNANDEZ said she was MARTINEZ's girlfriend and had let MARTINEZ drive the white Toyota Tacoma pick-up truck a couple times in the past few days. FERNANDEZ was also aware that MARTINEZ committed robberies in Taos, Española, and Santa Fe, NM. On August 14, 2022, FERNANDEZ took MARTINEZ to Taos, NM, and on August 15, 2022, FERNANDEZ picked up MARTINEZ from the Family Dollar and Dollar General after the robberies were committed.

21. FERNANDEZ had the Device in her possession during the interview. She gave the USMS and Espanola Police Department consent to review the Device. She unlocked the Device using her fingerprint. The Device can also be unlocked with a pattern but FERNANDEZ did not remember the pattern. During a review of the Device, officers observed messages between FERNANDEZ and MARTINEZ discussing the robberies and communicating pickup times. A picture of a revolver matching the description of the silver revolver used in the commission of crimes was found on the Device. Subsequently EPD detained FERNANDEZ and seized FERNANDEZ's Device.

22. Therefore, while the Espanola Police Department might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws

23. The Device is currently in storage at EPD, 1316 Calle Adelante, Espanola, NM 87532. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the EPD.

24. Based on my training knowledge and experience I have reason to believe that the Device contains relevant data regarding violations of Title 18 United States Code (U.S.C.) §§ 1951, Interference with Commerce by Threats and Violence (Hobbs Act), and 922(g)(1) and 924, Felon in Possession of a Firearm and involving MARTINEZ and FERNANDEZ. Specifically, communications about the planning and execution of the robberies, location data tying FERNANDEZ to the scene of the robberies, photographs of items used or worn during the commission of the robberies, and discussion of motive for the commission of the robberies.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video,

or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing

computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://www.samsung.com/us/smartphones/galaxy-a32-5g/, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and Pager with access to the Internet and potential to store IP addresses. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer

a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric

passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, if a locked device is equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

f. I know that FERNANDEZ enabled at least one biometric passcode—her fingerprint—on the Device.

31. Based on the foregoing, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe FERNANDEZ's fingers (including thumbs) to the fingerprint scanner of the Device; (2) hold the Device in front of FERNANDEZ's face and activate the facial recognition feature, for the purpose of attempting to unlock the Device in order to search its contents as authorized by this warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B for violations of 18 U.S.C. §§ 1951, 922(g)(1), and 924.

34. This affidavit was reviewed and approved by AUSA Mark Pfizemayer.

Respectfully Submitted,

Emily Pertitta
Special Agent
Federal Bureau of Investigation

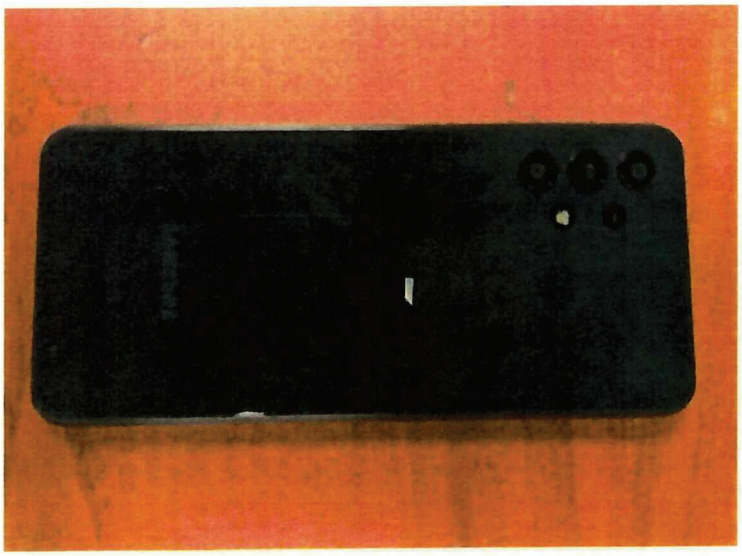
Subscribed and sworn to before me by telephone
On August ~~XX~~ 19, 2022. - JHR

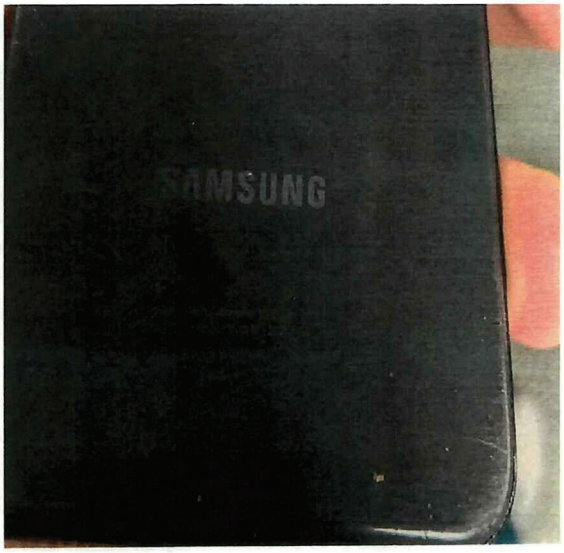
THE HONORABLE JERRY H. RITTER, U.S. MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Samsung Galaxy, IMEI 357157887221312, cracked screen black/dark gray color, hereinafter the "Device." The Device is currently located at the Espanola Police Department, 1316 Calle Adelante, Espanola, NM 87532.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.





ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18 United States Code (U.S.C.) §§ 1951, Interference with Commerce by Threats and Violence (Hobbs Act), and 922(g)(1) and 924, Felon in Possession of a Firearm and involving MARTINEZ and FERNANDEZ since August 9, 2022 including but not limited to:

a. any data about or related to the possession, purchase, sale, trade, or ownership of firearms and ammunition.

b. photographs or records of currency obtained during the commission of the Hobbs Act violations.

c. any information of plans made to conduct robberies and coordinate travel.

d. searches for robbery locations and plans for getaway routes.

e. any information related to items used or clothing worn during the commission of the crimes.

f. any information recording MARTINEZ's and FERNANDEZ's schedule or travel from August 9, 2022 to the present.

g. Any conversations between FERNANDEZ and MARTINEZ any another person about the robberies, including but not limited to phone calls, voicemails, text messages, and multimedia messages.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the Device described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who was in possession of the Device, to the fingerprint scanner of the device; (2) hold the Device in front of the face those same individual(s) and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.